

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-273856
(43)Date of publication of application : 26.09.2003

(51)Int.Cl. H04L 9/08
G09C 1/00
H04J 11/00
H04J 13/00
H04Q 7/38

(21)Application number : 2002-069516

(71)Applicant : COMMUNICATION RESEARCH LABORATORY
TEKTRONIX JAPAN LTD

(22)Date of filing : 14.03.2002

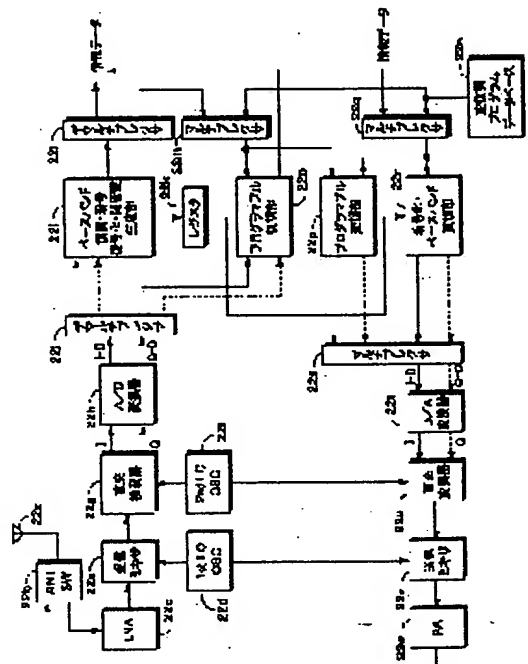
(72)Inventor : HONDA MAKOTO
HARADA HIROSHI
FUJISE MASAYUKI

(54) COMMUNICATION APPARATUS AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide radio transmission for information or program data with higher secrecy, without the need of private key transmission.

SOLUTION: A received digital baseband signal is supplied to a baseband demodulation/cipher decryption/private key generation unit 22j or a programmable demodulation unit 22o. At the baseband demodulation/cipher decryption/private key generation unit 22j, a private key for decryption of a demodulation/error correction codes and for encryption and cipher decryption is generated, and cipher decryption is conducted to output the decrypted cipher as information data or a modulation/demodulation program. According to the modulation/demodulation program, a modulation/demodulation device of the desired specification is configured. Transmission information data or program is processed for encryption, error correction encoding, and digital modulation by the private key at an encryption/baseband modulation unit 22r. The encryption/baseband modulation unit 22r outputs baseband digital data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-273856

(P2003-273856A)

(43) 公開日 平成15年9月26日 (2003.9.26)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-コ-ド ⁷ (参考)
H 0 4 L 9/08		G 0 9 C 1/00	6 5 0 B 5 J 1 0 4
G 0 9 C 1/00	6 5 0	H 0 4 J 11/00	5 K 0 2 2
H 0 4 J 11/00		H 0 4 L 9/00	6 0 1 A 5 K 0 6 7
13/00		H 0 4 B 7/26	1 0 9 R
H 0 4 Q 7/38		H 0 4 L 9/00	6 0 1 E

審査請求 未請求 請求項の数16 OL (全 23 頁) 最終頁に続く

(21) 出願番号 特願2002-69516 (P2002-69516)

(22) 出願日 平成14年3月14日 (2002.3.14)

(71) 出願人 301022471

独立行政法人通信総合研究所

東京都小金井市貫井北町4-2-1

(71) 出願人 000108409

日本テクトロニクス株式会社

東京都品川区北品川5丁目9番31号

(72) 発明者 本多 真

東京都品川区北品川5丁目9番31号 ソニ

ー・テクトロニクス株式会社内

(74) 代理人 100082762

弁理士 杉浦 正知

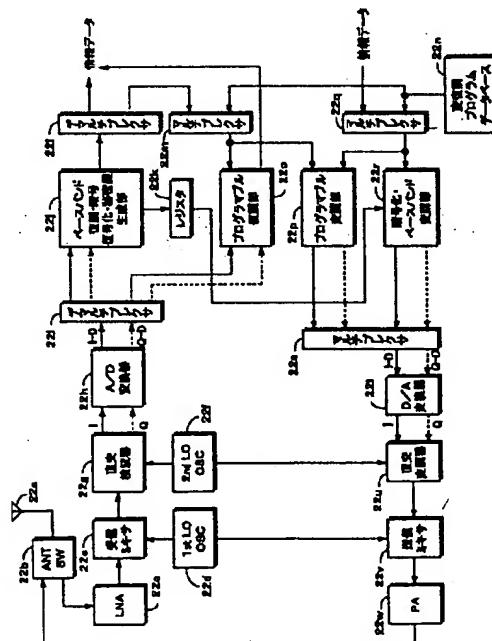
最終頁に続く

(54) 【発明の名称】 通信装置および通信方法

(57) 【要約】

【課題】 秘密鍵を伝送する必要がなく、高い機密性で情報またはプログラムデータを無線伝送する。

【解決手段】 受信デジタルベースバンド信号がベースバンド復調・暗号復号化・秘密鍵生成部22jまたはプログラマブル復調部22oに供給される。ベースバンド復調・暗号復号化・秘密鍵生成部22jにおいては、復調・誤り訂正符号の復号化、さらに、暗号化と暗号復号化のための秘密鍵が生成され、暗号の復号化が行われて情報データまたは変復調プログラムとして出力される。変復調プログラムにしたがって所望の仕様の変復調器が構成される。送信情報データまたはプログラムが秘密鍵によって暗号化・ベースバンド変調部22rにおいて暗号化、誤り訂正符号化、デジタル変調の処理を受ける。暗号化・ベースバンド変調部22rは、ベースバンドデジタルデータを出力する。



【特許請求の範囲】

【請求項1】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置。

【請求項2】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置。

【請求項3】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置。

【請求項4】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置。

【請求項5】 請求項1、2、3または4において、他の通信装置から受信した受信信号中の上記既知の信号に基づいて、上記伝搬路の遅延プロファイルまたは上記周波数特性を推定する通信装置。

【請求項6】 請求項1、2、3または4において、内部に既知の信号を使用して伝搬路の伝達関数を推定し、上記伝達関数の逆特性を実現する等化器を備え、上記等化器で決定されたフィルタ係数に基づいて上記秘密鍵を生成する通信装置。

【請求項7】 請求項1、2、3または4において、上記既知の信号がパイロットシンボルであり、上記伝搬路の遅延プロファイルまたは上記周波数特性を推定する手段は、内部にパイロットシンボルをそれぞれ含む、送信パケットと上記受信データパケットとが時間的に隣接して配され、上記受信データパケット中の上記パイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。

【請求項8】 請求項1、2、3または4において、上記既知の信号がパイロットシンボルであり、送信データパケットおよび受信データパケットにそれぞれ上記パイロットシンボルが含まれ、上記送信データパケットと上記受信データパケットとが時間的に隣接して配され、上記受信データパケット中の上記パイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。

【請求項9】 請求項1、2、3または4において、上記既知の信号がパイロットシンボルであり、送信および受信するデータパケットと別個に上記パイロットシンボルのスロットを形成し、送信するパイロットシンボルと受信するパイロットシンボルとを時間的に隣接したスロットに配し、受信したパイロットシンボルを使用して上記遅延プロファイルまたは上記周波数特性を推定する通信装置。

【請求項10】 請求項1、2、3または4において、上記既知の信号としてPN系列を使用する通信装置。

【請求項11】 請求項1、2、3または4において、さらに、平文に対して第1の誤り検出符号で符号化を行い、第1の誤り検出符号のパリティを有するデータに対して暗号化を行い、暗号化されたデータに対して第2の誤り検出符号で符号化を行う通信装置。

【請求項12】 請求項1、2、3または4において、受信データは、送信側において、平文に対して第1の誤り検出符号で符号化がされ、上記第1の誤り検出符号のパリティを有するデータに対して暗号化がなされ、暗号化されたデータに対して第2の誤り検出符号で符号化がされており、

上記第2の誤り検出符号の復号化を行い、復号結果が合

格であれば、上記秘密鍵を使用して復号化を行い、上記第1の誤り検出符号の復号化を行い、復号結果が合格であれば、復号化データとして出力する通信装置。

【請求項13】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける無線通信システムにおける通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定するステップと、

推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なうステップとを有する通信方法。

【請求項14】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の周波数特性を推定するステップと、

推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いて情報データを暗号化して送信し、または上記秘密鍵で暗号化された情報データを受信して復号化を行なうステップとを有する通信方法。

【請求項15】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法であって、

ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬路の遅延プロファイルを推定するステップと、

推定した上記遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なうステップとを有する通信方法。

【請求項16】 略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信方法であって、

ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信方法において、

既知の信号に基づいて、上記他の通信装置との間の伝搬

路の周波数特性を推定するステップと、

推定した上記周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成するステップと、

上記秘密鍵を用いてプログラムデータを暗号化して送信し、または上記秘密鍵で暗号化されたプログラムデータを受信して復号化を行なうステップとを有する通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、無線通信システムにおける通信装置および通信方法に関する。

【0002】

【従来の技術】近年、普及の著しい携帯電話や無線LAN(Local area network)を始めとする移動体無線通信システムは社会の最も重要なインフラの一つと見なすことができる。当然のことであるが、例えば企業や情報機密および個人のプライバシー保護の観点から無線の盗聴を防止するためには暗号化は必須である。

【0003】一方、近年、ソフトウェア無線通信システムの研究開発が活発に行なわれている。ソフトウェア無線通信システムとは、無線通信システムをデジタル化してソフトウェアでシステム機能を変更することにより、単一のハードウェアでも複数のシステム機能に対応できるマルチモードのシステムを実現するという概念である。ソフトウェア無線通信システムによれば、通信装置の仕様・規格、動作特性などを使用する環境に応じて変更することが可能となり、また、各種の通信方式や異なる規格がプログラムを書き換えるだけで一つの装置で使用できるようになるため、開発費用の削減、期間の短縮、大量生産及び、保守・更新への適合性、低コスト化を実現できる。

【0004】より具体的には、ソフトウェア無線通信技術では、マイクロプロセッサやDSP(Digital Signal Processor)のチップまたはFPGA(Field Programmable Gate Array)を用いてデジタル無線通信用のプログラマブルな変復調装置を構成し、所望の通信方式の変復調方式を構成するためのソフトウェアを変復調装置にインストールして、種々の仕様を同一のハードウェアで柔軟に実現することができる。例えばソフトウェアをインストールすることによって、PHS(Personal Handyphone System)や携帯電話、構内LAN(Local Area Network)等の異なる無線通信方式を1つの無線通信装置で実現することができれば、ユーザは同一の無線端末装置さえあればその地域の通信方式のプログラムをインストールすることによって世界中でサービスを受けられる。端末装置の製造メーカーにとっては、ハードウェアを共通化することによって量産が可能となり、製造コストを削減できる。

【0005】ところで、ソフトウェア無線通信システム

において、共通のハードウェア上に種々のプログラムを搭載して対応した無線通信方式に基づく無線通信装置を実現するためには、ソフトウェアのインストール方式としては、電話や、有線インターネット等の有線によってケーブルを接続してダウンロードする方法（第1の方法）、超小型のメモリデバイスによる方法（第2の方法）、無線によってプログラムをダウンロードする方法（第3の方法）が考えられる。

【0006】第1の方法は、自宅、職場、販売店、駅・空港等の公共施設にソフトウェア供給装置を設けて利用者のソフトウェア無線端末装置をケーブルで接続して有線経由でダウンロードする方法である。第1の方法は、利用者はソフトウェア供給装置のある場所を探し、足を運ばなければならない問題点を有する。第2の方法は、販売店などで所望のソフトウェアが格納されているメモリデバイスを購入する必要がある。媒体であるメモリデバイスの価格が高くなってしまふ。第3の方法は、前述した第1および第2の方法と異なり利用者が電波の届く場所にいれば、所望のプログラムを伝送して効率よくダウンロードできる。そこで、以降は無線経由でプログラムの伝送・ダウンロードを行なう無線ダウンロードの方式に着目する。

【0007】ソフトウェア無線機が動作するのに必要とされるプログラムは、メーカーが作成して政府の電波を管理する部署が電波法を満たすかどうかを検査して、その検査に合格し、販売を認可されたプログラムでなければならない。例えば、そのプログラムに意図的な改竄が行なわれた場合、インストールしたソフトウェア無線機が違法電波または妨害電波を発生してしまうことになり、無線通信インフラを破壊しかねない。あるユーザAに対してソフトウェアの無線ダウンロードが行なわれると仮定する。悪意のある別のユーザBがそのプログラムを盗聴しソフトウェア無線機にダウンロードしてユーザAになりすまして通信を行なってしまうことも有り得る。この場合では、ユーザAに経済的に多大な損害を与えることも考えられる。また、ユーザBが盗聴したプログラムを改竄して違法電波を発生することも有り得る。

【0008】以上のような情報データとソフトウェア無線通信システムにおけるプログラムの機密性を向上させるために、暗号化技術を適用する方法がある。従来の暗号化技術として、図1および図2に示すようなものが知られている。図1は一般的な公開鍵暗号方式の構成である。この方式の代表的な暗号はRSA (Rivest-Shamir-Adleman) 暗号がある。公開鍵と秘密鍵はともに整数値である。公開鍵は一般に公開されているが、一方、秘密鍵は公開されないため、暗号通信に先立って第三者に盗聴されないように配送されなければならない。図1において、参照符号1aが暗号通信で送信する予定の情報データまたはプログラムである。参照符号1bが暗号化アルゴリズムである。参照符号1cが伝送路であり、参照符

号1dが受信側における復号化アルゴリズムであり、復号化アルゴリズム1dは、受信した暗号化を復号化鍵すなわち秘密鍵を用いて、参照符号1eで示す情報データまたはプログラムを復号化する。

【0009】図2は、暗号化鍵および復号化鍵として、共に秘密鍵を使用する共通鍵方式または秘密鍵方式の構成を示す。この方式の代表的な例はDES (Data Encryption Standard) および、DEA (Data Encryption Algorithm) であり、それぞれ、ANSI (米国規格協会、American National Standards Institute) と ISO (国際標準化機構、International Organization for Standardization) で標準化されている。秘密鍵は送信側と受信側で同じ鍵を持たなければならないので、通信のペアの両者に同じ鍵を持たせるために、暗号通信に先立って第三者に盗聴されないように鍵を配送しなければならない。参照符号2aが暗号通信で送信する予定の情報データまたはソフトウェアである。参照符号2bが暗号化アルゴリズムである。参照符号2cは伝送路であり、参照符号2dは受信側における復号化アルゴリズムであり、復号化アルゴリズム2dは、受信した暗号化データを復号化鍵すなわち秘密鍵を用いて、参照符号2eで示す情報データまたはプログラムを復号化する。

【0010】

【発明が解決しようとする課題】従来の暗号化技術例えば秘密鍵方式を使用して、ソフトウェア無線通信システムにおける基地局では、秘密鍵を用いてプログラムに対して暗号化を施した後に端末局に伝送する。端末局では秘密鍵を用いて復号化の後、プログラムをダウンロードする。しかしながら、端末局側の秘密鍵の番号が漏洩し、悪意のある利用者がその秘密鍵を用いて暗号を解読し、プログラムを解析し、改竄の後に端末のハードウェアにインストールして違法電波を送信し、無線インフラを破壊する可能性がある。したがって、現在、信頼性の高い秘密鍵生成方法の確立が必要であると考えられる。

【0011】したがって、この発明の目的は、鍵配送の問題を生じることがなく、無線通信システムにおいて情報データ、ソフトウェア無線のプログラムデータ等を安全に通信することを可能とする通信装置および通信方法を提供することにある。

【0012】

【課題を解決するための手段】上述した課題を解決するために、請求項1の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いて情報データを暗号化して送信し、または秘密鍵で暗号化された情報データを受信して復号化

を行なう手段とを有する通信装置である。請求項13は、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【0013】請求項2の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いて情報データを暗号化して送信し、または秘密鍵で暗号化された情報データを受信して復号化を行なう手段とを有する通信装置である。請求項14の発明は、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【0014】請求項3の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の遅延プロファイルを推定する手段と、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いてプログラムデータを暗号化して送信し、または秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置である。請求項15の発明は、推定した遅延プロファイルの複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【0015】請求項4の発明は、略同一のキャリア周波数を時分割に使用して他の通信装置との間で送信および受信を交互に行なう無線通信システムにおける通信装置であって、ハードウェアの一部または全部がプログラム可能な論理回路で構成され、論理回路に対するプログラムデータによって、所望の無線通信方式を実現するようにした通信装置において、既知の信号に基づいて、他の通信装置との間の伝搬路の周波数特性を推定する手段と、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する手段と、秘密鍵を用いてプログラムデータを暗号化して送信し、または秘密鍵で暗号化されたプログラムデータを受信して復号化を行なう手段とを有する通信装置である。請求項16の発明は、推定した周波数特性の複素振幅情報、電力情報および位相情報の少なくとも一つを用いて、秘密鍵を生成する通信方法である。

【0016】この発明では、電波伝搬路の遅延プロファイルまたは周波数特性が二つの通信装置の間で固有の情報となることに着目し、二つの通信装置間の伝搬路の遅延プロファイルまたは周波数特性から暗号化の秘密鍵を生成する。秘密鍵を相手に伝送する必要がなく、高いセキュリティで無線通信を行うことができる。情報シンボルデータのみならず、ソフトウェア無線装置のプログラムデータも高いセキュリティでもって通信できる。

【0017】

【発明の実施の形態】この発明の一実施形態について以下説明する。基地局から端末局に情報データまたはプログラムを伝送する際に他局に盗聴されないような暗号用の秘密鍵を生成するためには、基地局と端末局の2者のみしか知らない固有の情報に着目すれば良い。ここで、基地局から端末局に対して送信される電波の下りのキャリアに周波数と端末局から基地局に対して送信される電波の上りのキャリア周波数は一致し、十分に短い時間間隔で上りと下りの電波が交互に繰り返されて送信されるものとする。

【0018】波長が数cm（通常1GHz以上）のマイクロ波、または数ミリ程度（30～300GHz）のミリ波を使用した場合、基地局と端末局の無線伝搬路の伝達関数または周波数特性は、その時刻と位置に依存した両者に固有のデータと成り得る。空間的にたかだか数cmの距離を移動するのみで無線伝搬路の特性が激変し、自己と周囲の移動物体によって特性は時々刻々と変動する。したがって、基地局と他の端末間の電波伝搬路の特性とは無関係であるとみなせるから、その無線伝搬路の特性から特徴量を抽出して、それに基づいて秘密鍵を生成すれば極めて機密性の高い暗号化を行うことができる。

【0019】図3は、陸上移動通信における電波伝搬の様子を示す。基地局3aと端末局3b間には、建造物、自動車や樹木が存在する。これらは電波が伝搬するうえで大きな影響を与える。屋外の基地局3aから送信された電波は唯一の通り道だけを通して伝搬するのではなく、あらゆる方向に放射され、移動局3bへ直接到来する直接波3cの他にビル3dによる反射波3e、自動車3fなどの移動物体による反射波3gが端末局3bに到達する。2局間には他にも電波が建造物の角などにより電波の進行方向が曲げられる回折波、建造物の角や壁面の不均一性などで電波があらゆる方向に散っていく錯乱波も無数存在する。これらの電波はそれぞれに経路長が異なるため、移動局に到達する時間が異なる。その結果として移動局では到達時間の異なるいくつもの電波（遅延波）の重ね合わせを受信することになる。これをマルチパルスと呼ぶ。

【0020】端末局や周囲の反射物が移動することにより激しいフェージングを伴った電波となる一般的な携帯電話のセルラ環境においては、フェージング特性がレイリー分布となることが解析的に導かれている。レイリー

フェージング下における受信信号の空間的な相関については空間で半波長程度離れた2本のアンテナで受信したフェージング信号は互いに無相関であると導かれている。例えば、キャリア周波数をそれぞれ、2GHzと5GHzとすれば $\lambda = 150\text{mm}$ 、 $\lambda = 60\text{mm}$ であるから、無相関であるための空間的なアンテナの距離はそれぞれ、75mmと30mmとなる。

【0021】電波の伝搬路特性は、時間領域で表される遅延プロファイルと、周波数特性で表現することができる。図4は、ある伝搬環境の遅延プロファイルの例を示す。遅延プロファイルは、基本的には、インパルス波形を地点Aから送信し、地点Bで受信したインパルス波形の電力の過渡応答を測定したものである。これは、電波の伝搬路の時間領域の伝達特性を表す。最初に、時刻が0のときに最も遅延が最小で受信電力が最大の直接波が到来して、続いて電力の減衰した反射波・回折波・錯乱波が伝搬距離に応じて遅れて到来することを示している。

【0022】マイクロ波とミリ波において、遅延プロファイルの波形は、受信地点とある時刻において固有の特性であり、数ミリから数センチのオーダーで離れた2つの受信地点で測定すれば、各受信地点における伝搬特性は無相関の異なった特性となる。つまり、伝搬路の遅延プロファイルの各時間に対応したパスの振幅と位相が異なる。この点に着目すれば、振幅と位相情報は、キャリア周波数、時刻、送信点並びに受信地点に固有のものであり、他の受信地点では得ることができない。したがって、この特性から基地局と端末局のみが共有する秘密鍵を生成することが可能となる。また、時間領域上の特性である遅延プロファイルを周波数領域に変換した周波数特性においても同様である。

【0023】インパルス波形は広帯域のスペクトラムを有するために他の無線通信に妨害を与えてしまうおそれがある。そこで、インパルス波を送信する代わりに、キャリアを自己相関特性の強い既知のPN(Pseudo Noise)信号(M系列とも呼ばれる)で変調し、被変調信号を送信する。受信側では、受信信号と同一のPN信号との相関演算を行なう。遅延プロファイルは、このような手法で測定することができる。

【0024】図5は、遅延プロファイル測定のための送信装置の構成例を示す。参照符号5aで示すPN系列発生器5aは、シフトレジスタと排他的論理和ゲートから構成されている。PN系列の出力ビットがBPSK(Binary Phase Shift Keying: 2相位相偏移変調)変調器5bによってBPSK変調される。BPSK変調器5bの出力のIチャンネル(同相成分)のデジタルデータI-DとQチャンネル(直交成分)のデジタルデータQ-DがそれぞれD/A変換器5cによってベースバンドアナログ信号に変換される。直交検波器5dにおいて、ベースバンドアナログ信号が第1局部発振器5eの発振

周波数の中間周波数帯信号に変換される。その後に送信ミキサ5fと第2局部発振器5gによってキャリア周波数に変換され、パワーアンプ5hで電力増幅を行なった後にアンテナ5iから送信される。

【0025】図6は、遅延プロファイル測定のための受信装置の構成例を示す。ディジタル変調されたキャリアをアンテナ6aより受信し、ローノイズアンプ6bで受信波の信号増幅を行なう。ローノイズアンプ6bの出力信号が受信ミキサ6cに供給され、受信ミキサ6cにおいて、第1局部発振器6dの出力信号と乗算されることによって中間周波数帯信号に変換される。直交検波器6eと第2局部発振器6fによって中間周波数帯信号は、IチャンネルとQチャンネルから構成されるベースバンド信号に変換される。A/D変換器6gによって両チャンネルのベースバンドアナログ信号がそれぞれディジタルデータに変換される。各チャンネルのディジタルデータが複素数相関器6hに入力される。送信装置で使われたのと同種のPN発生器6iがBPSK変調器6jによって変調され、BPSK変調器6jからのディジタル変調信号と受信信号との複素数相関演算が複素数相関器6hにおいて行われ複素遅延プロファイルとして出力される。

【0026】図7は、測定された複素遅延プロファイルの一例を示す。各グラフの横軸は遅延時間を表す。図7Aおよび図7Bは、それぞれ複素遅延プロファイルの振幅の実数成分の時系列データ7aと虚数成分の時系列データ7bを示す。図7Cおよび図7Dは、それぞれ複素数の振幅情報から計算した電力の時系列データ7cと位相の時系列データ7dを示す。

【0027】次に、電波の伝搬路の周波数特性について説明する。周波数特性は、図7Aおよび図7Bに示すような複素遅延プロファイルの振幅の時系列複素数データをDFT(Discrete Fourier Transform)またはFFT(Fast Fourier Transform)によって周波数領域の複素数データに変換したものである。図8は、FFTを使用した場合の計算手法を示す。図6に示した受信装置の複素遅延プロファイルの出力をシリアル・パラレル変換器8aによってFFTのポイント数のパラレルデータに変換してFFT8bに入力する。FFT8bが伝搬路の周波数特性を出力する。なお、図面において、実線の信号経路が実数データの信号経路を表し、破線の信号経路が虚数データの信号経路を表している。

【0028】以上の説明では、図5に示した送信装置と、図6に示した受信装置とを使用した自己相関特性の良好なPN信号を使用した遅延プロファイルの測定システムについて説明した。次に、PN信号を使用しない一般的な既知信号を使用した伝搬路の周波数特性の測定手法について述べる。送信側では、図5のPN発生器5aとBPSK変調器5bの代わりにディジタル変調された既知信号が生成され、既知信号が送信される。

【0029】一方、受信側では、A/D変換された複素デジタルデータに対して、図6中の複素数相関器6h、PN発生器6i、BPSK変調器6jに代えて図9に示す構成が設けられる。受信した時間領域の既知信号の複素デジタルデータ $x(t)$ がシリアル・パラレル変換器9aによってパラレルデータに変換され、FFT9bによって周波数領域のパラレルデータ $X(f)$ に変換される。あらかじめ用意した既知信号データ $y(t)$ 9cがシリアル・パラレル変換器9dによってパラレルデータに変換され、変換したパラレルデータをFFT9eに入力して周波数領域データ $Y(f)$ に変換する。 $X(f)$ を $Y(f)$ で複素除算することによって伝搬路の周波数特性 $Z(f)$ を求めることができる。すなわち、 $Y(f)Z(f)=X(f)$ の関係にあり、 $Z(f)=X(f)/Y(f)$ となる。

【0030】図10は、伝搬路の周波数特性の例を示す。各グラフの横軸は周波数を示す。図10Aおよび図10Bは、それぞれ振幅の実数成分10aと虚数成分10bを示す。図10Cおよび図10Dは、複素振幅のデータから計算した電力の特性10cと位相の特性10dをそれぞれ示す。

【0031】図7に示した複素遅延プロファイルと、図10に示した伝搬路の周波数特性は、例えば、5GHzのキャリア周波数を使用して測定したとすれば、受信アンテナの空間的な距離が30mm以上差れていればそれぞれの受信地点での特性は無相関であるとみなせる。また受信地点と送信地点を交換しても同一周波数で且つ測定時刻が十分に近ければ可逆性が成立し、送信側と受信側のアンテナや増幅器などの利得を考慮して正規化すれば同様な特性が得られる。したがって、伝搬路の複素遅延プロファイルと周波数特性は送信側と受信側の両者だけのキャリア周波数と位置と時刻に依存する固有の特性であるとみなせる。それらの特性をある手法に基づいて数値化すれば、送信側と受信側が共有する秘密鍵を生成することが可能となる。以下に、伝搬路の遅延プロファイルと周波数特性の電力、振幅、位相の各情報による秘密鍵生成の手法を示す。

【0032】図11は、電力情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の電力のパラレルデータがM入力N出力選択器11aに入力される。M入力N出力選択器11aは、M個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいN個のデータを選択して出力する。図7の遅延プロファイルの例では、 $t_0, t_1, t_2, \dots, t_N$ のそれぞれの時刻のそれぞれの振幅がM個のデータである。この選択器11aで選択されたN個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器11bに入力されて秘密鍵が生成される。

【0033】図12は、振幅情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の振幅

のパラレルデータがM入力N出力選択器12aに入力される。M入力N出力選択器12aは、M個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいN個のデータを選択して出力する。この選択器12aで選択されたN個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器12bに入力されて秘密鍵が生成される。

【0034】図13は、位相情報から秘密鍵を生成する構成を示す。遅延プロファイルまたは周波数特性の位相のパラレルデータがM入力N出力選択器13aに入力される。M入力N出力選択器13aは、M個の遅延プロファイルまたは周波数特性の複素パラレルデータの中で、電力が比較的大きいN個のデータを選択して出力する。この選択器13aで選択されたN個の遅延プロファイルまたは周波数特性の複素パラレルデータが電力・秘密鍵生成器13bに入力されて秘密鍵が生成される。

【0035】図14は、M入力N出力選択器の構成例を示す。 $M \geq N$ とする。M個の入力複素数データはそれぞれ電力計算回路14a₁~14a_Nに入力されて電力が計算される。例えば入力データ番号が1の入力データの実数データ a_1 と虚数データ b_1 とから、電力計算回路14a₁は、 $(a_1^2 + b_1^2)$ の演算によって電力を計算する。計算した電力値がマルチプレクサ制御信号生成器14bに入力されて電力の比較的高いN個の入力複素数データを選択する制御信号が生成される。この制御信号がN個のマルチプレクサ14c₁~14c_Nに供給される。マルチプレクサ14c₁~14c_Nに対しては、M個の入力複素数データが供給され、制御信号にしたがってその中の一つが選択的に出力される。マルチプレクサ14c₁~14c_Nによって選択したN個の入力複素数データが出力される。

【0036】図11、図12、図13にそれぞれ示された電力情報、振幅情報、位相情報から秘密鍵を生成する秘密鍵生成器11b、12b、13bの構成についてさらに説明する。

【0037】図15は、電力・秘密鍵生成器11bの構成例を示す。N個の複素数データはそれぞれ電力計算回路15a₁~15a_Nによって電力が計算される。計算した電力値は多入力加算器15bに入力され電力和が求められる。その電力和に対して除算器15cによってデータ個数Nで除算が行われて平均電力が算出される。この平均電力値を用いて各入力データの電力値を除算器15d₁~15d_Nでそれぞれ除算して正規化を行なう。正規化した各データに対して量子化回路15e₁~15e_Nによって量子化が行われ、それぞれpビットのビット系列に割り当てられる。入力されたN個のビット系列はビット結合器15fによって結合されてNpビットの秘密鍵として出力される。

【0038】図16は、図15で使用した電力計算回路15a₁~15a_Nの構成例を示す。入力された実数デー

タと虚数データを2乗回路16a、16bでそれぞれ2乗した後に加算器16cで加算して電力値として出力する。

【0039】図17は、図15で使用した量子化回路15e₁~15e_Nの動作例を示す。ここではp=3、すなわち、3ビット出力の例を示す。入力された正規化された電力値に対応するビット系列を出力する。レベル範囲の境界上の白い丸は、その値を範囲内に含まないことを意味し、黒い丸は、その値を範囲内に含むことを意味する。例えば、正規化電力値として4.5が入力された場合、出力ビット系列として(101)が出力される。

【0040】図18は、ビット結合器の構成例を示す。量子化されて変換されたN個のデータ系列のビット数をそれぞれpとすれば、それらを結合してNpビットのデータとして出力される。例えば、p=3として1番目のデータを(100)、2番目のデータを(001)、3番目のデータを(010)、N番目のデータを(111)とすれば、ビット結合器の出力は(100001010, ..., 111)となる。

【0041】図19は、図12で使用した振幅・秘密鍵生成器12bの構成例を示す。N個の複素振幅データの実数成分が多入力加算器19aに入力され、多入力加算器19aによって実数成分の振幅値の総和が求められ、また、虚数成分が多入力加算器19bに入力され、多入力加算器19aによって虚数成分の振幅値の総和が求められる。実数成分の総和が除算器19cに供給され、虚数成分の総和が除算器19dに供給され、各除算器19c、19dによって各総和をデータ入力数Nで割って実数と虚数のそれぞれの平均振幅値が求められる。

【0042】求めた平均振幅値によって実数入力データと虚数入力データがそれぞれ正規化される。除算器19e₁~19e_Nによって、N個の実数入力データのそれぞれが実数成分の平均振幅値で除算されることで、正規化がなされる。同様に、除算器19f₁~19f_Nによって、N個の虚数入力データのそれぞれが虚数成分の平均振幅値で除算されることで、正規化がなされる。正規化された実数データが実数の量子化回路19g₁~19g_Nによってpビットのビット系列にそれぞれ変換され、ビット結合器19iに入力される。同様に、正規化された虚数データが虚数の量子化回路19h₁~19h_Nによってpビットのビット系列にそれぞれ変換され、ビット結合器19iに入力される。実数データおよび虚数データがビット結合器19iによって結合されて2Npビットの秘密鍵として出力される。なお、図19における量子化回路とビット結合器の構成は、図17と図18で示した構成とそれぞれ同様である。

【0043】図20は、位相・秘密鍵生成器13bの構成例を示す。N個の複素数データはそれぞれ位相・ビット変換器20a₁~20a_Nによって位相値からpビットのビット系列に変換されてビット結合器20bに入力さ

れて結合されたNpビットのビット系列が秘密鍵として出力される。ビット結合器の構成は図18と同様である。図20で図示はしないが、N個の複素数データから直接、位相・ビット変換する手法のほかに、例えば入力データ番号が1の複素数データの位相を基準位相 θ_{ref} と定め、N個の複素数データから求めた位相値から θ_{ref} を引いた相対的な位相値を用いてビットに変換する手法も考えられる。

【0044】図21は、位相・ビット変換器20a₁~20a_Nの動作例を示す。図21Aに示す例では、入力された複素数データを(p=1)ビットに変換する例である。位相を θ とすると、($\pi/2 < \theta \leq \pi$, $-\pi/2 \leq \theta < -\pi$)では、 θ が0に変換され、($0 < \theta \leq \pi/2$, $-\pi/2 < \theta \leq 0$)では、 θ が0に変換される。図21Bに示す例では、実数軸(横軸)および虚数軸(縦軸)で表される2次元領域の4つの象限に含まれる位相がそれぞれ(p=2)ビットへ変換される。図21Cに示す例では、2次元領域が45°の各間隔で8個の領域に分割され、各領域に含まれる位相がそれぞれ(p=3)ビットへ変換される。なお、図21Bと図21Cにおいて、黒い丸はその境界を範囲内に含むことを意味し、白い丸はその値を範囲内に含まないことを意味する。

【0045】上述したように、遅延プロファイルと伝搬路の周波数特性が測定(推定)され、測定(推定)された遅延プロファイルまたは伝搬路周波数特性から秘密鍵が生成される。次に、無線通信装置に対して、これらの手法を適用した例について説明する。

【0046】図22は、上述した秘密鍵生成方式によるソフトウェア無線通信装置の構成例を示す。上部は復調部、下部は変調部である。本構成では、情報データのみならず所望の変復調器を構成するためのプログラムをも暗号化して無線伝送を行なう。プログラムの暗号化と暗号復号化のための秘密鍵をこの発明による方式で生成するものとする。復調部では、アンテナ22aから受信された信号はアンテナスイッチ22bを通り、ローノイズアンプ22cに入力される。ローノイズアンプ22cから出力された信号は、受信ミキサ22eにおいて、第1局部発振器22dの局部発振信号によって中間周波数帯信号に変換される。

【0047】中間周波数帯信号は、直交検波器22gにおいて、第2局部発振器22fの出力信号により直交検波され、アナログベースバンド信号I、Qに変換される。アナログベースバンド信号I、Qは、A/D変換器22hにおいて、ディジタルベースバンド信号I-D、Q-Dに変換される。ディジタルベースバンド信号I-D、Q-Dがデマルチプレクサ22iに供給される。ディジタルベースバンド信号I-D、Q-Dがデマルチプレクサ22iを介してベースバンド復調・暗号復号化・秘密鍵生成部22jまたはプログラマブル復調部22o

に供給される。

【0048】ベースバンド復調・暗号復号化・秘密鍵生成部22jにおいては、復調・誤り訂正符号の復号化、さらに、暗号化と暗号復号化のための秘密鍵が生成され、暗号の復号化が行われてマルチプレクサ22iを通して情報データまたは変復調プログラムとして出力される。復調された変復調プログラムは、マルチプレクサ22mを介してプログラマブル変調部22pとプログラマブル変調部22rに供給され、復調された変復調プログラムにしたがって、所望の仕様の変復調器が構成される。さらに、生成された秘密鍵はレジスタ22kに記憶される。

【0049】次に変調部の動作を説明する。マルチプレクサ22qから出力される情報データまたはプログラムは、まず、既に生成した秘密鍵が保持されているレジスタ22kから秘密鍵を読み出して、暗号化・ベースバンド変調部22rにおいて暗号化、誤り訂正符号化、デジタル変調の処理を受ける。暗号化・ベースバンド変調部22rは、ベースバンドデジタルデータとしてI-DとQ-Dを出力する。これらのデータは、マルチプレクサ22sを介してD/A変換器22tによってそれぞれ、ベースバンドアナログI、Q信号に変換される。

【0050】アナログ信号は、第2局部発振器22fの発振周波数の中間周波数帯に直交変調器22uによって変換される。中間周波数帯のアナログ信号は、送信ミキサ22vに供給され、送信ミキサ22vにおいて、第1局部発振器22dの発振周波数が加算されることで所望のキャリア周波数帯に変換される。この信号が電力増幅器22wによって電力が増幅された後にアンテナスイッチ22bを通りアンテナ22aによって送信される。

【0051】プログラマブル変調部22pとプログラマブル復調部22oは、デジタル信号処理をプログラムで行なうDSP(Digital signal processor)とプログラム可能な論理回路であるFPGA(Field programmable gate arrays)から構成されている。プログラマブル変調部22pとプログラマブル復調部22oの機能を拡張することが可能で、デジタル変復調のみならず、誤り訂正符号化・復号化機能や暗号化・暗号復号化機能も実現可能である。マルチプレクサ22i、22sを制御することによって、ベースバンド復調・暗号復号化・秘密鍵生成部22jと暗号化・ベースバンド変調部22rの代わりにこれらのプログラマブルな変調部と復調部が前述した機能を実現することもできる。

【0052】また、変復調プログラムデータベース22nには、自己で使用するプログラムと相手局に無線で伝送するプログラムが格納されている。マルチプレクサ22mは、プログラマブル変調部22pと復調部22oに対して無線伝送されたプログラムとデータベースのプログラムのどちらをダウンロードするかを選択する。マルチプレクサ22qは、情報データとデータベースのプロ

グラムのどちらを送信するかを選択する。なお、プログラムは、基地局に限らず、端末局が送信する機能を持つことも可能である。また、変復調プログラムデータベース22nを基地局のみが備えていても良い。

【0053】図23は、暗号化・ベースバンド変調部22rの構成例を示す。情報データ入力または変復調プログラム入力が入力された暗号化器23aによって暗号化され、誤り訂正符号化器23bによって符号化される。誤り訂正符号化器23bの出力がマルチプレクサ23cを介してベースバンドデジタル変調部23dに供給され、変調部23dによってデジタル変調され、ベースバンドデジタル変調データI-DとQ-Dが出力される。

【0054】伝搬路の遅延プロファイルと周波数特性の推定を行なうために、マルチプレクサ23cには、パイロットシンボルが入力され、一定周期でパイロットシンボルが挿入されたデータがデジタル変調される。ベースバンドデジタル変調方式は、例えば、無線LANで使用されているOFDM(Orthogonal frequency-division multiplexing)変調方式、スペクトル拡散変調方式さらに、一般の携帯電話等で使用されているシングルキャリア変調方式等である。なお、図23では、パケット生成ブロック等の図示を省略した。

【0055】以下では、図23におけるベースバンド復調・暗号復号化・秘密鍵生成部22jの内部構成に関して、OFDM変調方式、スペクトル拡散変調方式、シングルキャリア変調方式の3種類の方式について説明を行なう。

【0056】図24にこの発明による秘密鍵生成器を搭載したOFDM用ベースバンド復調・暗号復号化・秘密鍵生成部の第1の構成例を示す。図24中のスイッチ24e、24fは、それぞれ伝搬路特性推定モードと復調モードとで切り換えるものである。つまり、スイッチ24e、24fが復調モードでは、1の状態とされ、伝搬路特性推定モードでは、2の状態とされる。切り換え信号は、省略されているが、制御部から各スイッチに供給される。スイッチ24e、24fによって、FFTを伝搬路特性推定モードと復調モードとで兼用できる。

【0057】入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部24aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドデジタルデータに対してキャリア周波数同期部24bにおいてキャリア周波数を同期させる。同期させた後にシリアル・パラレル変換器24cにおいてシリアルデータからFFTの演算ポイント数の個数のパラレル複素数データに変換される。FFT24dにおいて入力された信号を周波数領域に変換し、周波数領域の信号をスイッチ24e、24fに供給する。

【0058】スイッチ24e、24fが1の状態では、通常のOFDM復調処理を行なう。スイッチが24e、

24fが2の状態では、受信した信号からパイロットシンボルを抽出して伝搬路の周波数特性の推定を行なう。伝搬路周波数特性の推定手法は図9に説明した手法を使用している。パイロットシンボルは既知であるから同様にパイロットシンボルをあらかじめFFTによって周波数領域に変換した参照データ24hが具備されている。

【0059】受信したパイロットシンボルをFFT24dによって変換された周波数領域の信号に対して、複素数除算器24gによって除算を行ない、伝搬路の周波数特性を計算する。その周波数特性から秘密鍵生成器24iによって秘密鍵を生成してレジスタ24kに記憶させる。この秘密鍵生成器24iは、図11、図12および、図13に示した構成に対応する。秘密鍵の生成手法は、図11から図22において説明したものである。周波数特性はレジスタ24jに記憶される。

【0060】スイッチ24e、24fが1の状態では、このレジスタ24jに記憶された伝搬路周波数特性を利用して等化器（複素数除算器）24lにおいて等化が行われる。等化器24lの出力がパラレル・シリアル変換器24mによってシリアルデータに変換されて誤り訂正符号復号化器24nに供給されて誤り訂正符号の復号化が行われる。さらに、生成した秘密鍵を用いて暗号復号化器24oにおいて暗号が復号化された後に情報ビットが出力される。また、生成した秘密鍵は変調部に出力される。

【0061】図25にはこの発明による秘密鍵生成器を搭載したOFDM用ベースバンド復調・暗号復号化・秘密鍵生成部の第2の構成例を示す。入力されたベースバンド複素デジタルデータに対しパケットタイミング同期部25aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドデジタルデータに対してキャリア周波数同期部25bにおいてキャリア周波数を同期させる。同期させた後にシリアル・パラレル変換器25cにおいてシリアルデータからFFTの演算ポイント数の個数のパラレル複素数データに変換される。FFT25dにおいて入力された信号が周波数領域の複素数データに変換される。このデータは等化器25eによって等化が行われた後にパラレル・シリアル変換器25fにおいてシリアルデータに変換される。そして、誤り訂正符号復号化器25gによって誤り訂正が行われ、その後に暗号復号化器25hに供給される。暗号復号化器25hでは、あらかじめレジスタ25mに記憶した秘密鍵を使用して暗号の復号化が行われ、情報ビットが出力される。

【0062】次に秘密鍵の生成について説明する。受信したパイロットシンボルは複素数相関器25jにおいてあらかじめ具備されている共役パイロットシンボル25iと相関演算が行われる。共役は、虚数部の符号が反転した関係を意味する。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変

換器25kにおいてパラレル複素数データに変換された後に秘密鍵生成器25lに供給される。秘密鍵生成器25lによって秘密鍵が生成される。この生成器の構成は図11、図12および、図13に示した構成例に対応する。生成した秘密鍵がレジスタ25mに記憶されて、暗号復号化器25hと変調部へ出力される。

【0063】図26にはこの発明による秘密鍵生成器を搭載したスペクトル拡散方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第1の構成例を示す。入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部26aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンド複素デジタルデータに対してキャリア周波数同期部26bにおいてキャリア周波数を同期させる。同期させた後、逆拡散・等化器26cによって逆拡散と等化が行われる。その出力に対して誤り訂正符号復号化器26dによって誤り訂正符号の復号化が行われて、暗号復号化器26eにおいてあらかじめ生成されたレジスタ26jに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【0064】次に、秘密鍵の生成について説明する。ベースバンド複素デジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器26gにおいてあらかじめ具備されている参照パイロットシンボル26fと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータがシリアル・パラレル変換器26hにおいてパラレルデータに変換された後に秘密鍵番号生成器26iによって秘密鍵が生成される。この生成器の構成は図11、図12および、図13に示した構成例に対応する。生成した秘密鍵はレジスタ26jに記憶されて、暗号復号化器26eと変調部へ出力される。また、推定した遅延プロファイルは逆拡散・等化器26cにも供給される。

【0065】図27にはこの発明による秘密鍵生成器を搭載したスペクトル拡散方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第2の構成例を示す。入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部27aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンド複素デジタルデータに対してキャリア周波数同期部27bにおいてキャリア周波数を同期させる。同期させた後、逆拡散・等化器27cによって逆拡散と等化が行われる。その出力に対して誤り訂正符号復号化器27dによって誤り訂正符号の復号化が行われて、暗号復号化器27eにおいてあらかじめ生成されたレジスタ27kに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【0066】次に、秘密鍵の生成について説明する。ベースバンド複素デジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相

関器27gにおいてあらかじめ具備されている共役パイロットシンボル27fと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータがシリアル・パラレル変換器27hにおいてFFTポイント数のパラレルデータに変換される。そのパラレルデータはFFT27iによって周波数領域に変換されて伝搬路の周波数特性が計算される。伝搬路の周波数特性から秘密鍵生成器27jによって秘密鍵が生成される。その生成器の構成は図11、図12および図13に示した構成に対応する。生成した秘密鍵はレジスタ27kに記憶されて、暗号復号化器27eと変調部へ出力される。また、推定した遅延プロファイルは逆拡散・等化器27cにも供給される。

【0067】図28にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号器・秘密鍵生成部の第1の構成例を示す。入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部28aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドデジタルデータに対してキャリア周波数同期部28bにおいてキャリア周波数を同期させる。同期させた後、等化器28cによって等化が行われる。その出力に対して誤り訂正符号復号化器28dによって誤り訂正符号の復号化が行われて、暗号復号化器28eにおいてあらかじめ生成されレジスタ28jに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【0068】次に、秘密鍵の生成について説明する。ベースバンド複素デジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器28gにおいてあらかじめ具備されている共役パイロットシンボル28fと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変換器28hにおいてパラレルデータに変換された後に秘密鍵生成器28iによって秘密鍵が生成される。この生成器の構成は図11、図12および、図13に示した構成に対応する。生成した秘密鍵はレジスタ28jに記憶されて、暗号復号化器28eと変調部へ出力される。また、推定した遅延プロファイルは等化器28cにも供給される。

【0069】図29にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第2の構成例を示す。入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部29aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドデジタルデータに対してキャリア周波数同期部29bにおいてキャリア周波数を同期させる。同期させた後、等化器29cによって等化が行われる。その出力に対して誤り訂正符号復号化器29dによって誤り訂正

符号の復号化が行われて、暗号復号化器29eにおいてあらかじめ生成されレジスタ29kに記憶されている秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【0070】次に、秘密鍵の生成について説明する。ベースバンド複素デジタルデータよりパイロットシンボルを抽出する。受信したパイロットシンボルは複素数相関器29gにおいてあらかじめ具備された共役パイロットシンボル29fと相関演算が行われる。演算結果が遅延プロファイルとなる。遅延プロファイルのデータはシリアル・パラレル変換器29hにおいてパラレルデータに変換される。そのパラレルデータがFFT29iによって周波数領域に変換されて伝搬路の周波数特性が計算される。伝搬路周波数特性から秘密鍵生成器29jによって秘密鍵が生成される。この生成器の構成は図11、図12および、図13に示した構成に対応する。生成した秘密鍵はレジスタ29kに記憶されて、暗号復号化器29eと変調部へ出力される。また、推定した遅延プロファイルは等化器29cにも供給される。

【0071】図30にはこの発明による秘密鍵生成器を搭載したシングルキャリア方式用ベースバンド復調・暗号復号化・秘密鍵生成部の第3の構成例を示す。入力されたベースバンド複素デジタルデータに対してパケットタイミング同期部30aでタイミングの同期をとり、同期パルスを各部に供給する。また、入力されたベースバンドデジタルデータに対してキャリア周波数同期部30bにおいてキャリア周波数を同期させる。同期させた後、等化器30cによって等化が行われる。その出力が誤り訂正符号復号化器30dによって誤り訂正符号の復号化が行われて、暗号復号化器30eにおいてあらかじめ生成されたレジスタ30gに記憶された秘密鍵を用いて暗号の復号化が行われて情報ビットが出力される。

【0072】次に、秘密鍵の生成について説明する。一般的な等化器は、内部にパイロットシンボルを具備し、そのシンボルを使用してある種の推定アルゴリズムによって伝搬路の伝達関数を推定し、その伝達関数の逆特性をFIR(Finite Impulse Response)フィルタで実現し、誤差が最小となるようにフィルタの係数を適応的に決定している。また、そのフィルタの係数は、その時刻における伝搬路の固有なパラメータであると考えられる。そこで、等化器30cのフィルタの係数データを秘密鍵生成器30fに供給して秘密鍵を生成する。その生成器の構成は図11、図12および、図13に示した構成に対応する。生成した秘密鍵はレジスタ30gに記憶されて、暗号復号化器30eと変調部へ出力される。

【0073】図31に図30の構成図内で使用する等化器30cの構成例を示す。等化器に供給された入力複素数データがレジスタ31a₁～31a_{N-1}が縦続接続されたシフトレジスタにサンプリングクロック毎に記憶される。レジスタ31a₁～31a_{N-1}の入力データおよび出

力データが係数生成部31cと複素数乗算器31b₁~31b_nに供給される。係数生成部31cでは、LMS (Least Mean Squares) アルゴリズムまたは、RLS (Recursive Least Squares) アルゴリズムによって係数が生成される。

【0074】係数生成部31cで生成された係数が複素乗算器31b₁~31b_nに供給され、計数出力C₁~C_nとレジスタ31a₁~31a_{n-1}の入出力データとの積が生成される。この積が複素数多入力加算器31dに入力される。加算器31dの出力がスイッチ31e、31fに入力される。スイッチ31e、31fが1の状態に設定された場合では、通常の等化器として動作が行われ、等化された結果として出力される。一方、パイロットシンボルを受信・入力した場合は、スイッチ31e、31fが2の状態に設定され、フィルタ係数の計算が行なわれる。このとき、加算器31dの出力がスイッチ31e、31fを介して減算器31g、31hに入力され、あらかじめ具備されているパイロットシンボル31iとの誤差が計算される。誤差は、係数生成部31cに供給される。係数生成部31cは、その誤差が最小となるような最適な係数C₁~C_nを計算する。また、その係数C₁~C_nが秘密鍵生成のために出力される。この生成器の構成は、図11、図12および図13に示した構成に対応する。

【0075】図32は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第1の構成例を示す。端末局から基地局に伝送される上りパケット32a₁、32a₂、...と基地局から端末局に伝送される下りパケット32b₁、32b₂、...が同一のキャリア周波数で交互に伝送される。上りパケットおよび下りパケットの両パケットのデータ構成について説明する。

【0076】1パケットは、パイロットシンボル32c、誤り検出を行なうCRC (Cyclic Redundancy Check) 符号によるパリティビット32d、暗号化された情報データ32eから構成される。情報データは、情報シンボル32f₁、32f₂、...32f_nから構成されている。CRCは、受信時にパリティビットチェックを行ない、誤りが検出された場合には、送信側に対して再送要求が行なわれる。なお、上りと下りパケットとは、基本的には同じ構成である。

【0077】図33は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第2の構成例を示す。当然のことながら基地局と端末局で生成した秘密鍵は本来、一致していなければならない。しかしながら、雑音または高速に移動する移動通信の伝搬環境下において伝搬路の状態が激変することによって両者で推定した伝搬路特性に差異が生じて生成した秘密鍵が異なる可能性がある。本構成は、基地局と端末局で生成した秘密鍵が異なった場合、それを検出・再生成させる

ための機能を付加したものである。

【0078】端末局から基地局に伝送される上りパケット33a₁、33a₂、...と基地局から端末局に伝送される下りパケット33b₁、33b₂、...が同一のキャリア周波数で交互に伝送される。上りおよび下り両パケットの内部構成について説明する。パイロットシンボル33c、誤り検出を行なうCRC符号によるパリティビットCRC133d、暗号化された情報データ33eから構成される。情報データはパリティビットCRC233f、情報シンボル33g₁、33g₂、...33g_nから構成されている。

【0079】CRC1は、受信時にパリティチェックを行ない、ビット誤りが検出された場合には再送要求が行われる。CRC2の機能について説明する。この発明によれば秘密鍵が基地局と端末局でそれぞれ生成されるが、伝搬環境によってはその秘密鍵は一致しない場合が有り得る。

【0080】そこで、図34に示すように、送信側では、例えば、基地局において、まず、ステップS1において、平文(元の情報データ)にパリティCRC2を付加する。ステップS2において、CRC2を付加したデータに対して、基地局で生成した秘密鍵KBを用いて暗号化を行なう。ステップS3において、パリティCRC1を付加した後に、ステップS4において変調し、端末局に送信する。

【0081】受信側では図35に示すように、端末局側ではまず、ステップS11において、通常のCRC1による検査を行なう。ステップS12では、検査の結果が合格か否かがチェックされる。合格が確認されれば、ステップS14において、端末局で生成した秘密鍵KTで暗号復号化を行なう。CRC1による検査が不合格の場合は、ステップS13において再送要求が行われる。

【0082】ステップS15では、復号化されたデータに対してCRC2を用いて検査を行なう。ステップS16では、検査の結果が合格か否かがチェックされる。合格が確認されれば、ステップS18において、復調されたデータが情報データとして出力される。

【0083】両局の秘密鍵が異なっていれば、復号されたデータは正しいデータではなくビット誤りが発生するので、ステップS16においてなされるCRC2による検査が不合格となる確率が高い。このときは、ステップS17において、両局に対して秘密鍵の再生成・再暗号化・再送処理を要求する。それによって、両局の秘密鍵が異なっていることを検出できる。

【0084】図36は、この発明による秘密鍵生成器を搭載した無線通信システムで使用するパケットの第3の構成例を示す。基地局と端末局の両局で生成した秘密鍵が一致しない一つの原因として、生成した時刻間の時間差によって伝搬路が変化して両者で推定した遅延プロファイルまたは周波数特性が異なってしまうことが挙げら

れる。そこで、その時間差を極力小さくする必要がある。

【0085】そこで、本パケット構成では、最初に、基地局が秘密鍵生成時に用いる上りパイロットシンボル36aを伝送し、その直後に直ちに端末局が秘密鍵生成時に用いる下りパイロットシンボル36bを伝送する。その後上りパケット36c₁、36c₂、・・・と下りパケット36d₁、36d₂、・・・が交互に伝送される。これらのパケットの内部構造は、図32または図33で示した構造と同様である。

【0086】図37は、図33、図34、図35、図36に示した手法によってパケットを構成した場合の送受信処理のタイムチャートを示す。まず、処理ST1では、端末局から基地局に向けて上りパイロットシンボル37aを送信する。基地局では直ちに下りパイロットシンボル37bを送信し、上りパイロットシンボルにより、伝搬路推定を行なって秘密鍵k_{B1}を生成する(ST2)。一方、端末局においても下りパイロットシンボルにより伝搬路推定を行なって秘密鍵k_{T1}を生成する(ST4)。

【0087】そして、秘密鍵k_{T1}を使用して情報データを暗号化して上りパケット37cとして送信する(ST5)。処理ST6において、基地局ではこのパケットのCRC1に対する検査を行ない、合格したと仮定する。次に、秘密鍵k_{B1}を使用して暗号復号化を行なった後にCRC2に対する検査を行ない、不合格であったと仮定する。k_{B1}とk_{T1}は等しくないと判断する。そして、基地局が秘密鍵の再生成のために下りパイロットシンボル37dを端末局に送信する(ST7)。

【0088】端末局において受信後、このパイロットシンボル伝送を秘密鍵の再生成の要求と判断して、秘密鍵k_{T2}を生成する(ST8)。直ちに上りパイロットシンボル37eを送信する(ST9)。基地局においてパイロットシンボル受信後に秘密鍵k_{B2}を生成する(ST10)。秘密鍵k_{B2}を用いて情報データを暗号化して下りパケット37fとして送信する(ST11)。

【0089】端末局側では、処理ST12において、CRC1とCRC2に対する検査がともに合格したと仮定する。これによって秘密鍵k_{T2}とk_{B2}が等しいと判断し、復号されたデータを情報データとみなす。次に、秘密鍵k_{T2}を用いて情報データを暗号化して上りパケット37gとして基地局に送信する(ST13)。基地局では、秘密鍵k_{B2}によって暗号復号化を行ない、復号されたデータを情報データとみなす(ST14)。以下、同様にパケットの送受を行なって、通信を行なう。なお、パイロットシンボルの送受を頻繁に行って秘密鍵を生成・更新する頻度を高めれば信頼性をさらに向上させることが可能となる。

【0090】この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱

しない範囲内で様々な変形や応用が可能である。例えば複素振幅情報、電力情報、位相情報の内の2以上の情報を使用して遅延プロファイルまたは周波数特性を推定するようにしても良い。また、図32、図33、または図36にそれぞれ示すデータ構成は、情報データに限らず、ソフトウェア無線装置のプログラムデータの通信に対しても適用できる。また、上述した構成において、各構成要素をハードウェア以外にソフトウェアによって実現するようにしても良い。さらに、この発明は、陸上移動通信に限らず、固定通信に対しても同様に適用でき、さらに、屋内の無線LANに対しても適用できる。

【0091】

【発明の効果】以上のように、この発明によれば、情報データまたはソフトウェア無線通信機のプログラムを2局間に固有の伝搬路の状態を利用して秘密鍵番号を生成することによって、盗聴が困難な秘匿性の高い秘密鍵を生成することが可能となる。一般的に陸上移動体通信等で用いられる周波数が数GHzものマイクロ波やミリ波においては特定の2局間の伝搬路状態は基地局と他の端末局間の無線伝搬路の状態とは無相関であるからである。この発明は、秘密鍵を送信側と受信側とで共有するために、相手側に秘密鍵を伝送することがなく、セキュリティを高くすることができる。

【図面の簡単な説明】

【図1】従来の暗号化方式の一例を示すブロック図である。

【図2】従来の暗号化方式の他の例を示すブロック図である。

【図3】陸上移動通信における電波伝搬の様子を示す略線図である。

【図4】遅延プロファイルの例を示す略線図である。

【図5】遅延プロファイル測定のための送信装置の構成例を示すブロック図である。

【図6】遅延プロファイル測定のための受信装置の構成例を示すブロック図である。

【図7】伝搬路の複素遅延プロファイルの例を示す略線図である。

【図8】伝搬路の周波数特性の求める処理の一例を示すブロック図である。

【図9】伝搬路の周波数特性の求める処理の他の例を示すブロック図である。

【図10】伝搬路の周波数特性の例を示す略線図である。

【図11】電力情報による秘密鍵生成方法を説明するためのブロック図である。

【図12】振幅情報による秘密鍵生成方法を説明するためのブロック図である。

【図13】位相情報による秘密鍵生成方法を説明するためのブロック図である。

【図14】M入力N出力選択器の構成例を示すブロック

図である。

【図15】電力・秘密鍵生成器の構成例を示すブロック図である。

【図16】電力計算回路の構成例を示すブロック図である。

【図17】量子化回路の構成例を示すブロック図である。

【図18】ビット結合器の構成例を示すブロック図である。

【図19】振幅・秘密鍵生成器の構成例を示すブロック図である。

【図20】位相・秘密鍵生成器の構成例を示すブロック図である。

【図21】位相・ビット変換器のいくつかの動作例を示す略線図である。

【図22】この発明をソフトウェア無線通信装置に適用した一実施形態のブロック図である。

【図23】この発明の一実施形態における暗号化・ベースバンド変調部の構成例を示すブロック図である。

【図24】この発明の一実施形態におけるOFDM用ベースバンド復調・暗号化復号化・秘密鍵生成部の第1の構成例を示すブロック図である。

【図25】この発明の一実施形態におけるOFDM用ベースバンド復調・暗号化復号化・秘密鍵生成部の第2の構成例を示すブロック図である。

【図26】この発明の一実施形態におけるスペクトラム拡散用方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第1の構成例を示すブロック図である。

【図27】この発明の一実施形態におけるスペクトラム拡散用ベースバンド復調・暗号化復号化・秘密鍵生成部

の第2の構成例を示すブロック図である。

【図28】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第1の構成例を示すブロック図である。

【図29】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第2の構成例を示すブロック図である。

【図30】この発明の一実施形態におけるシングルキャリア方式用ベースバンド復調・暗号化復号化・秘密鍵生成部の第3の構成例を示すブロック図である。

【図31】この発明の一実施形態におけるシングルキャリア復調器用等化器の構成例を示すブロック図である。

【図32】この発明で使用するバケットの構成の第1の例を示す略線図である。

【図33】この発明で使用するバケットの構成の第2の例を示す略線図である。

【図34】第2のバケット構成を使用した場合の送信側の処理を説明するフローチャートである。

【図35】第2のバケット構成を使用した場合の受信側の処理を説明するフローチャートである。

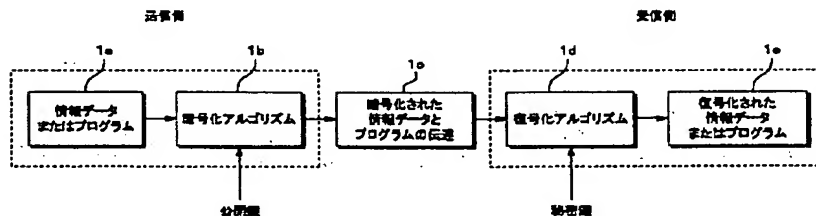
【図36】この発明で使用するバケットの構成の第3の例を示す略線図である。

【図37】この発明が適用された無線通信システムにおけるバケット通信のタイミングチャートである。

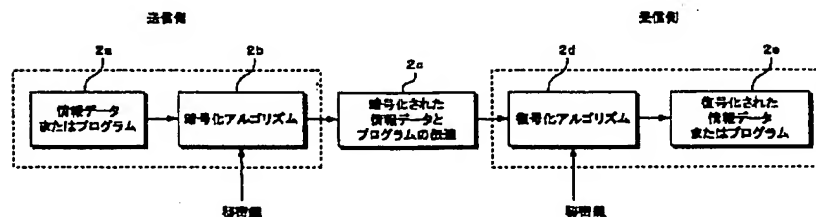
【符号の説明】

3 a . . . 基地局、3 b . . . 端末局、2 2 j . . . ベースバンド復調・暗号復号化・秘密鍵生成部、2 2 o . . . プログラマブル復調部、2 2 p . . . プログラマブル変調部、2 2 r . . . 暗号化・ベースバンド変調部、2 2 n . . . 変復調プログラムデータベース

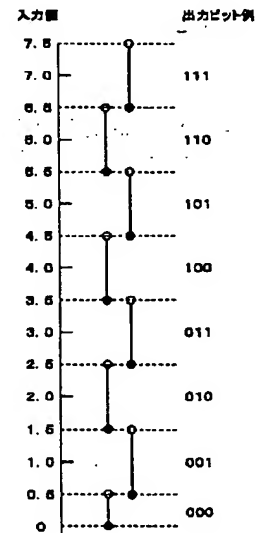
【図1】



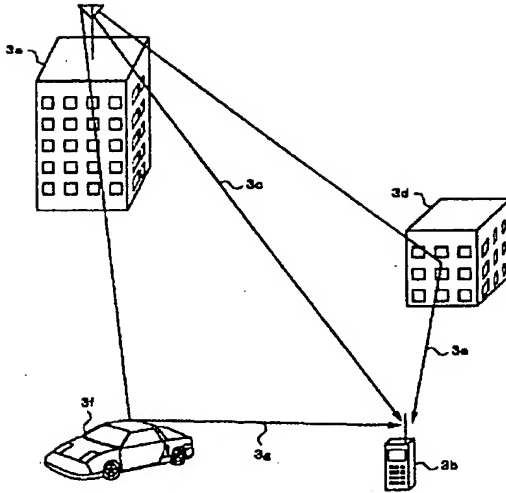
【図2】



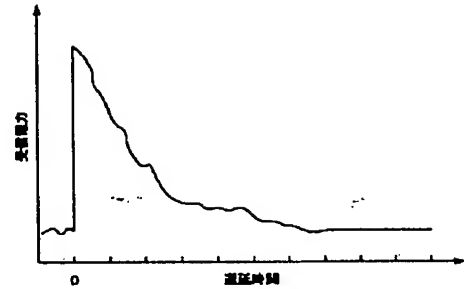
【図17】



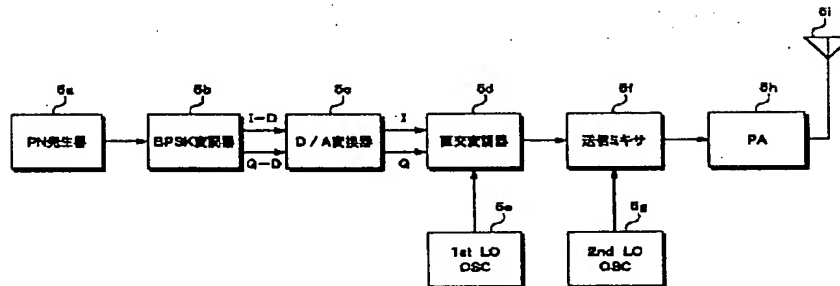
【図3】



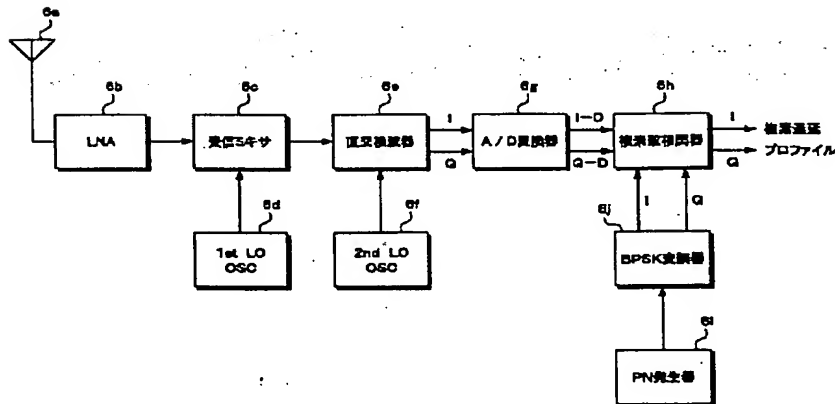
【図4】



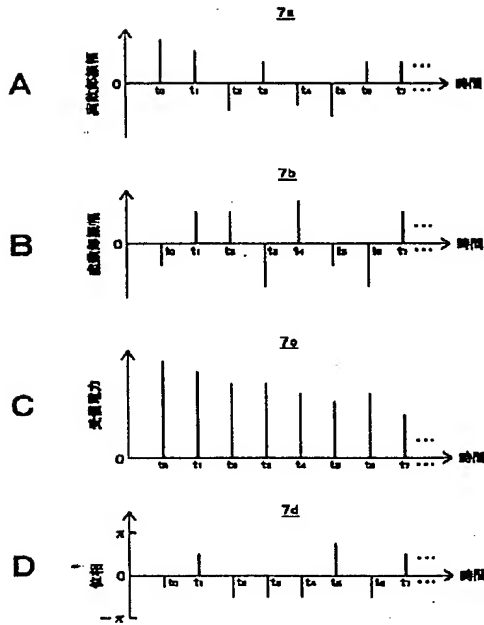
【図5】



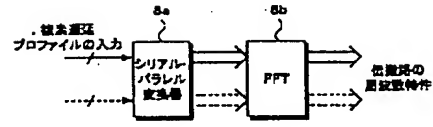
【図6】



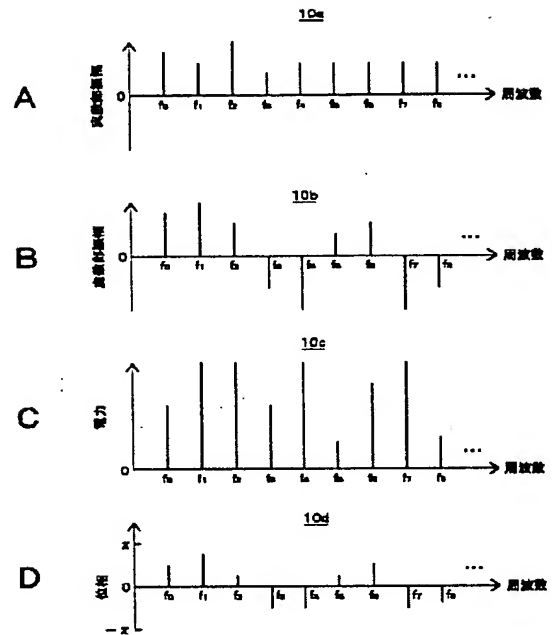
【図7】



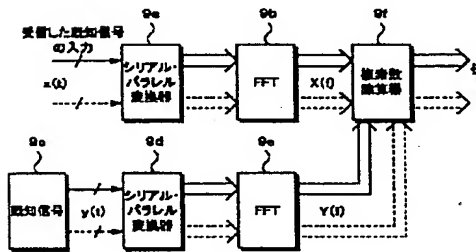
【図8】



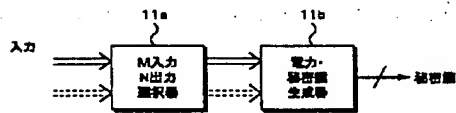
【図10】



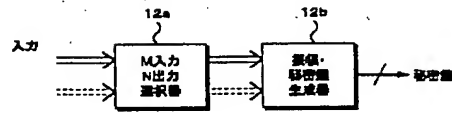
【図9】



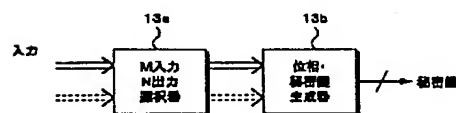
【図11】



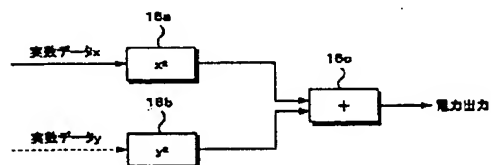
【図12】



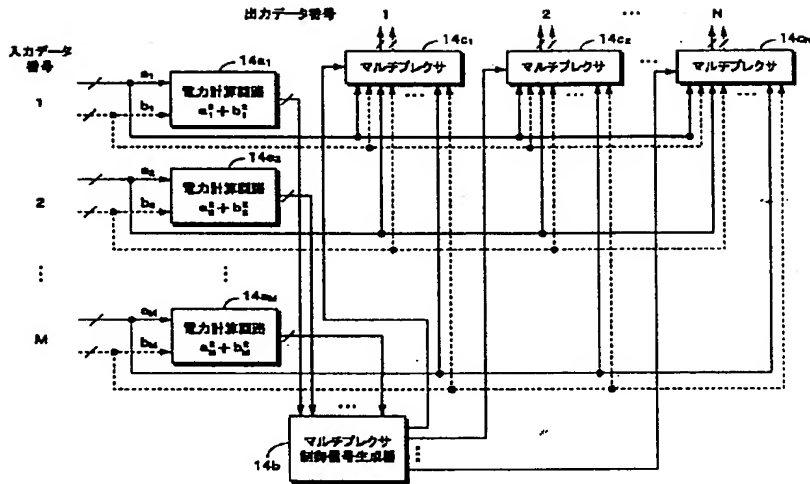
【図13】



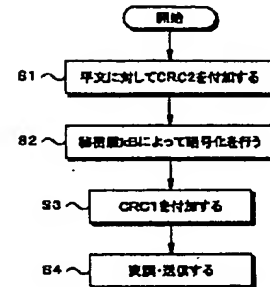
【図16】



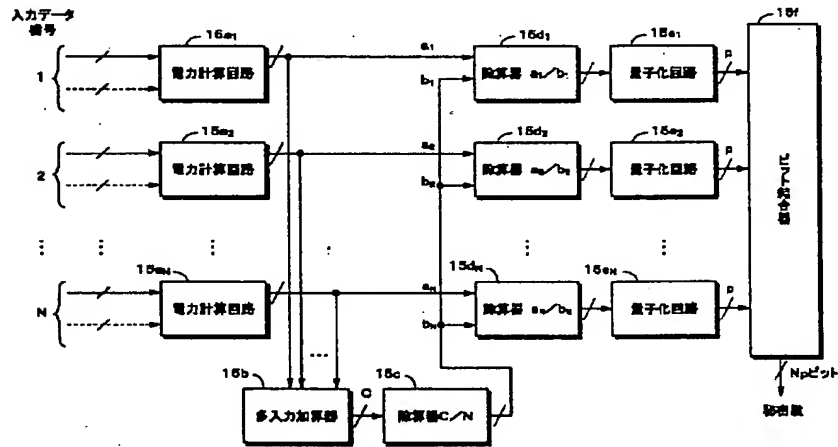
【図14】



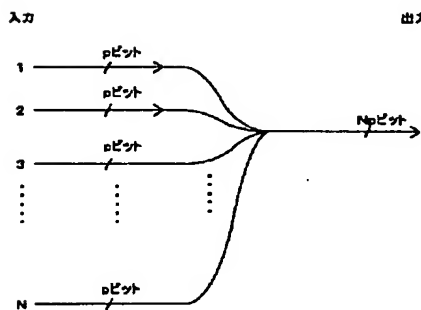
【図13】



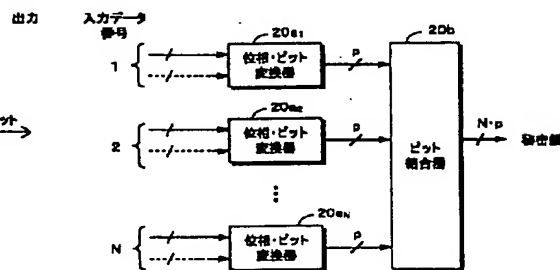
【図15】



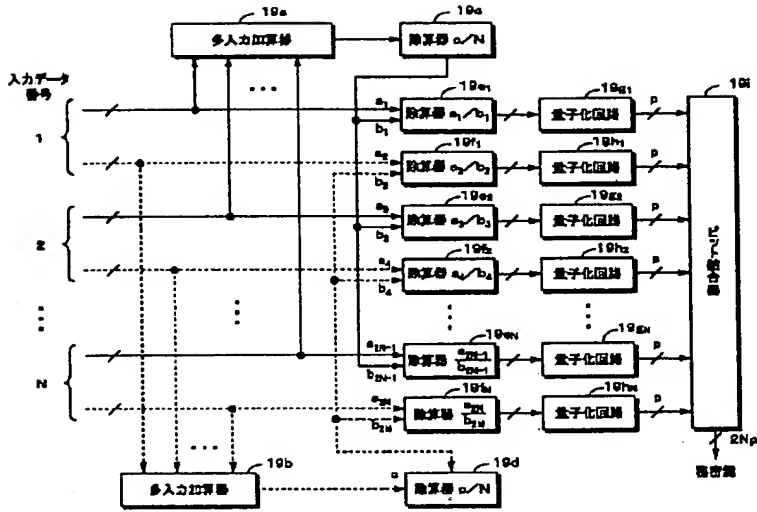
【図18】



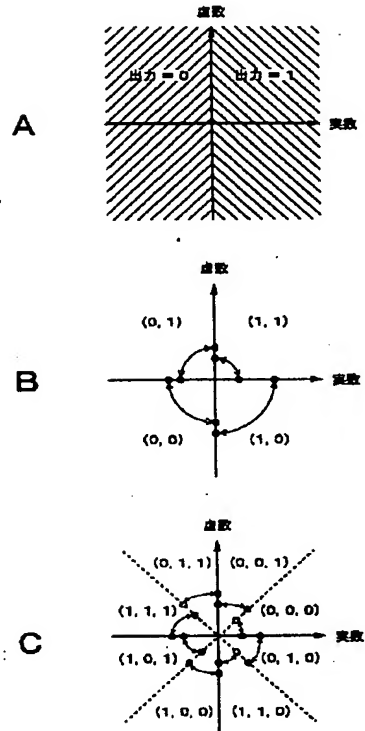
【図20】



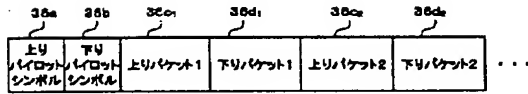
【図19】



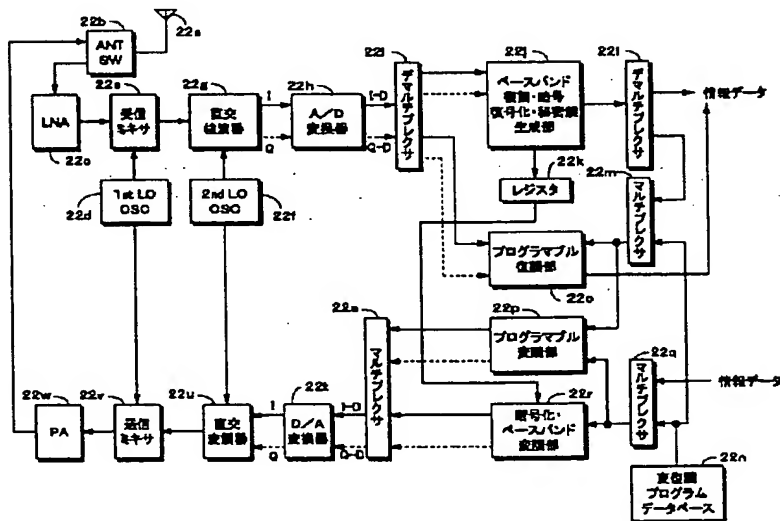
【図21】



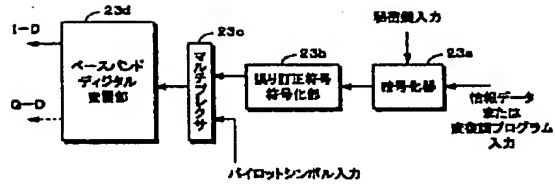
【図36】



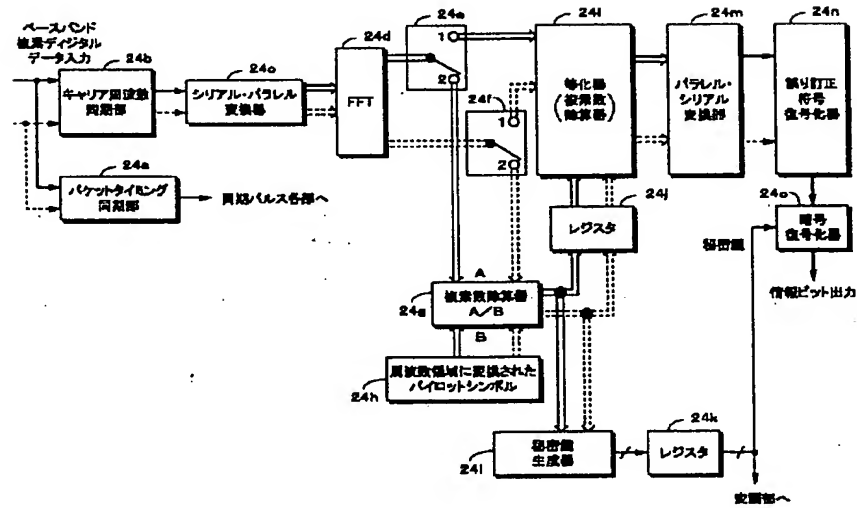
【図22】



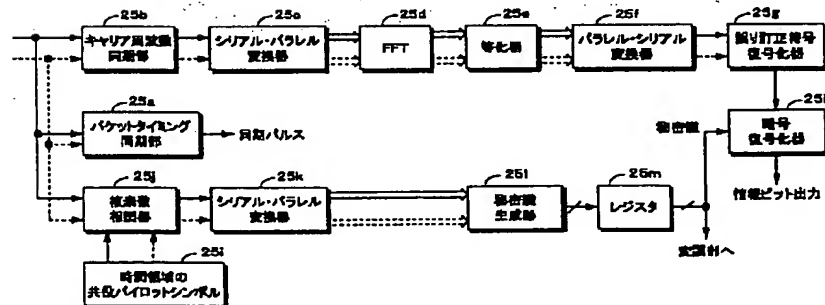
【例23】



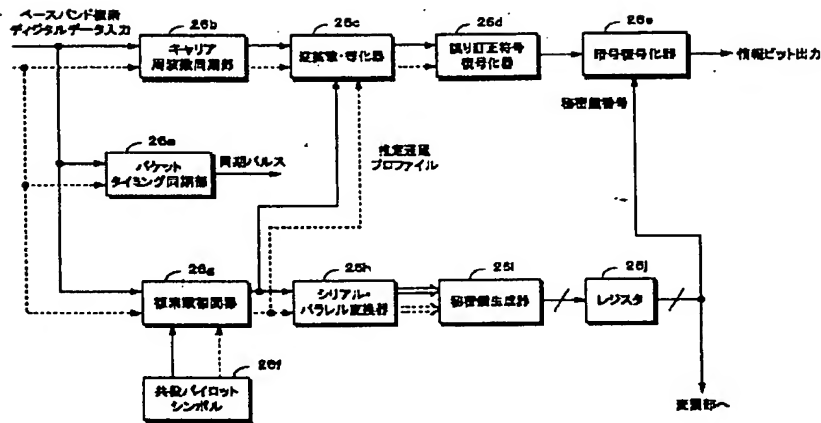
【図24】



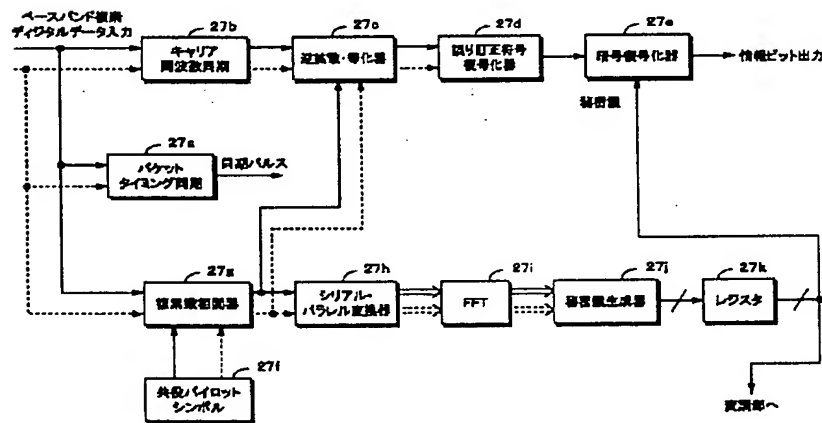
【图25】



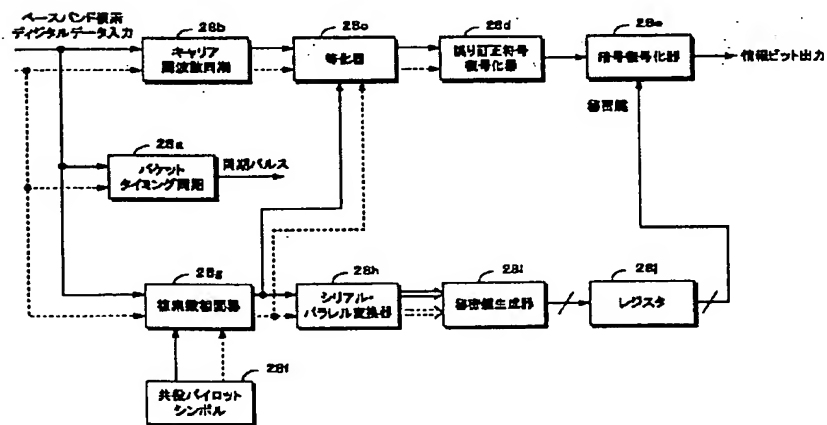
【図26】



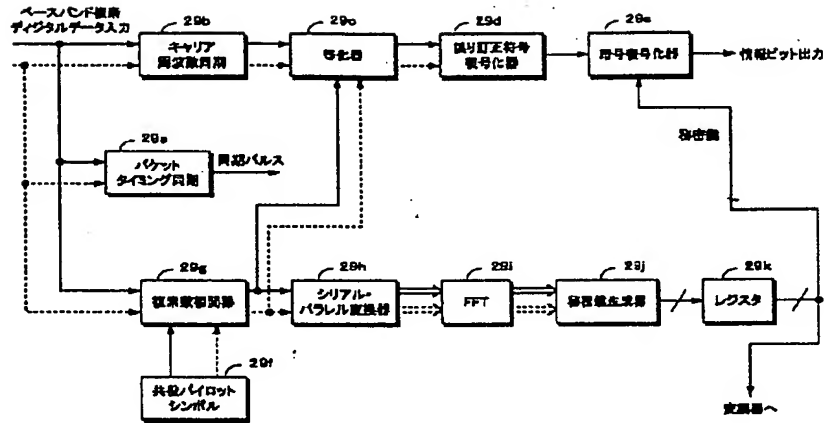
【図27】



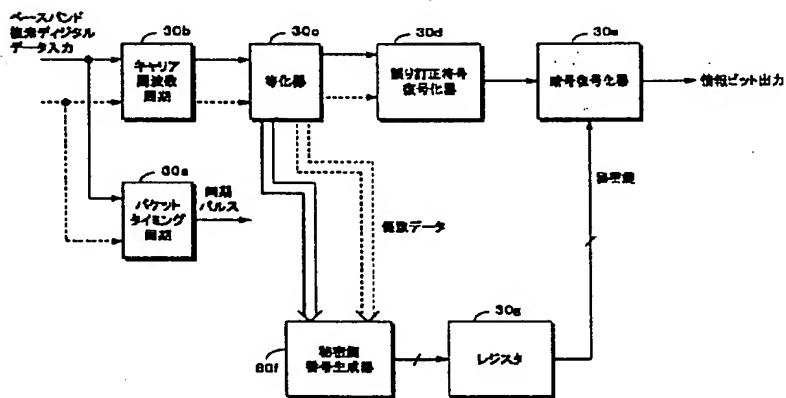
【図28】



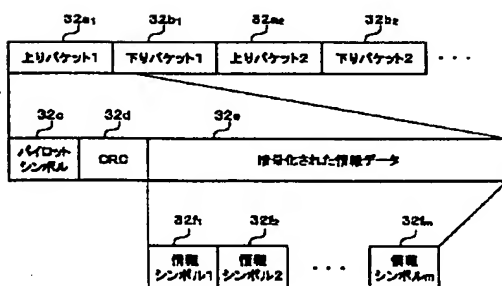
【図29】



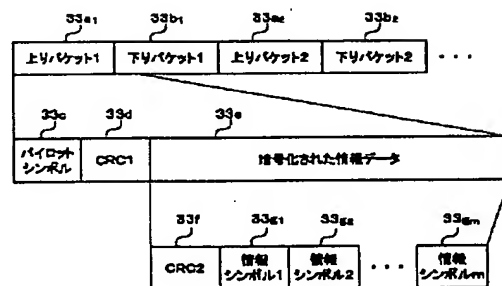
【図30】



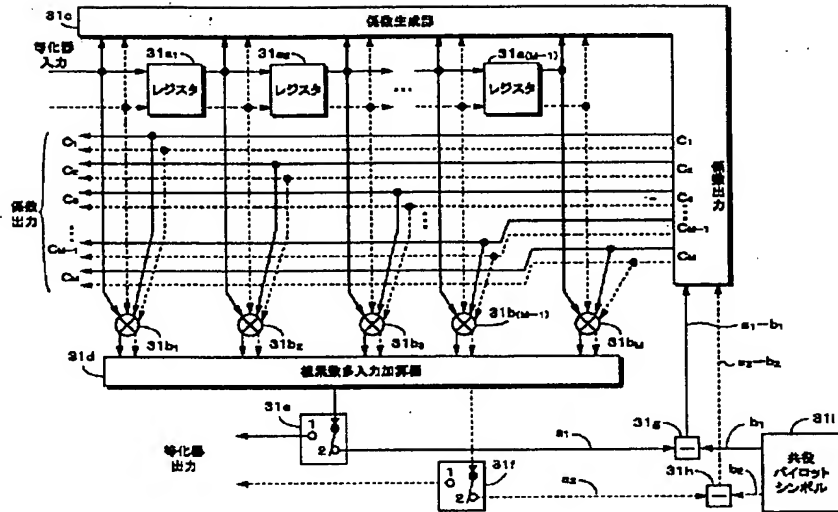
【図32】



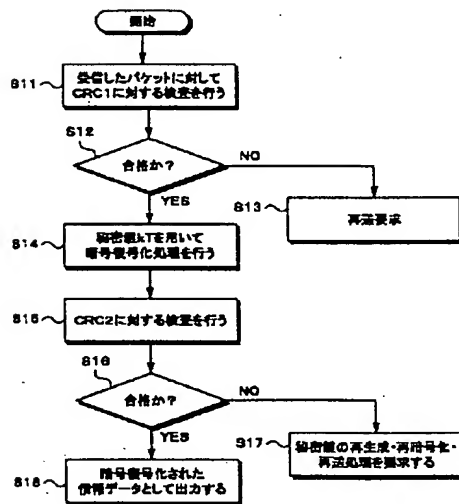
【図33】



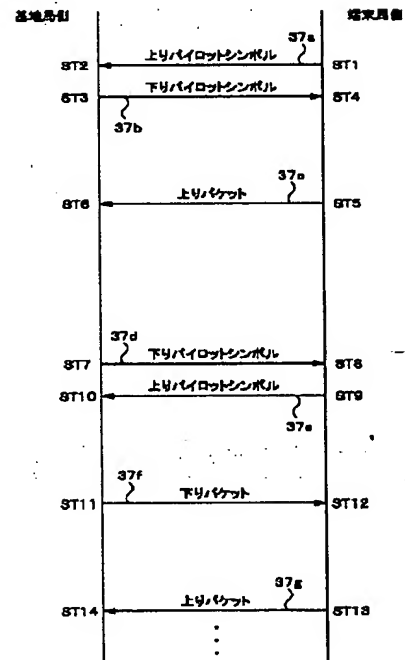
【図31】



【図35】



【図37】



(23) 03-273856 (P2003-27) 58

フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

H 0 4 J 13/00

キーワード(参考)

A

(72) 発明者 原田 博司

東京都小金井市貫井北町4-2-1 独立
行政法人通信総合研究所内

Fターム(参考) 5J104 AA16 EA04 EA24 JA03 NA02
PA01

5K022 DD01 DD13 DD19 DD23 DD33

(72) 発明者 藤瀬 雅行

東京都小金井市貫井北町4-2-1 独立
行政法人通信総合研究所内

EE02 EE14 EE22 EE32

5K067 AA30 AA33 BB04 BB21 CC04

DD17 HH36